Cisco Stealthwatch Cloud

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by Cisco Stealthwatch Cloud. Cisco Stealthwatch Cloud is in the process of being rebranded as Cisco Secure Cloud Analytics and is referred to herein as "Secure Cloud Analytics".

Secure Cloud Analytics is a cloud-based security solution made available by Cisco to companies or persons who acquire it for use by their authorized users.

In jurisdictions that distinguish between Data Controllers and Data Processors, Cisco is the Data Controller for the personal data processed to administer and manage the customer relationship. Cisco is the Data Processor for the personal data processed by Secure Cloud Analytics in order to provide its functionality.

1. Overview

Secure Cloud Analytics is a cloud security service that performs behavior anomaly detection on network connected devices and users on the customer premises and in public clouds to automatically detect early indicators of compromise such as insider threat activity, malware and multistaged attacks. Secure Cloud Analytics is a cloud-native, SaaS-delivered security and monitoring service that also identifies policy violations, misconfigured cloud assets and user error and misuse. Secure Cloud Analytics consumes logs and telemetry from customer IT environments (on-premises and public cloud), processes that IT telemetry, and produces security alerts in response to actionable security threats. Data and telemetry consumed by the services is metadata, i.e., which machines connected over the network, which users logged into which machines, etc. Secure Cloud Analytics does not collect the contents of network communications.

Secure Cloud Analytics offers identity and single sign-on through Auth0 and through Cisco SecureX Sign-On. Auth0 will no longer be available to new customers through Secure Cloud Analytics effective June 2021. For information regarding the processing of personal data by Cisco SecureX Sign-On, please see the SecureX Sign-On Privacy Data Sheet.

Secure Cloud Analytics integrates with various Cisco cloud services. For example, alerts raised in Secure Cloud Analytics can be pushed to a customer's Cisco WebEx portal to alert the appropriate customer team members. If you elect to enable integration between Secure Cloud Analytics and another Cisco cloud service or feature, you should also review the Privacy Data Sheet of such other cloud service or feature for information regarding the personal data collected, processed, and stored by that cloud service or feature.

Your Secure Cloud Analytics subscription includes access to Cisco SecureX, Cisco's integrated security platform that aggregates threat intelligence, unifies visibility across various Cisco and third-party security products, enables automated workflows, and more. For information regarding the processing of personal data by Cisco SecureX, please see the SecureX Privacy Data Sheet.

Cisco's Privacy Data Sheets are available here.

Secure Cloud Analytics also integrates with various third-party systems. Cisco is not responsible for customer data once it leaves Cisco Stealthwatch. Protection of data within the applicable third-party system is governed by the contract(s) and policies of the applicable third party.

Please see the following link for more details on Secure Cloud Analytics:
http://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html.

2. Personal Data Processing

The table below lists the personal data processed by Secure Cloud Analytics to provide its services and describes why the data is processed.

Personal Data Category	Type of Personal Data	Purpose of Processing
Account Information related to Portal Users	• User selected portal usernames (which could include names at the user's election) • Email addresses • Usage data (which may include usernames and/or IDs associated with actions taken in the Service)	• Account creation and service activation • Service authentication and log in • Product notifications • Authentication/authorization/license management • Deliver, support, upgrade and improve the service.
Network Flow Metadata	• Source IP address • Destination IP address	• Provide the security product functionality (i.e., threat and malware detection, identification of customer policy violations, misconfigured cloud assets and user error and misuse) and product improvements. • Cisco Talos and Cognitive Intelligence global threat intelligence research[1]
Other Metadata	Optional Additional Logs • User data • User ID • Username • User email address • User IP address • Device host name • Passive DNS logs Tags and Comments	• The customer has the option to elect to send additional logs containing user data for threat detection. This data is used only to provide the security product functionality. • Portal users have the option to add tags and comments related to security alerts. It is possible, but not recommended, that a portal user could add personal data related to the applicable security alert (e.g. the name of the employee associated with the alert). • Cisco Talos and Cognitive Intelligence global threat intelligence research[1]
Enhanced Network Flow Metadata for Encrypted Traffic Analytics (ETA)[2]	• Initial Data Packet ("IDP") which may include IP Header, TLS Header, SNI (Server Name Identifier), Ciphersuites (Certificate, Organization, Issuer, Issued, Expires)	• Security analytics, forensics, efficacy research, general product functionality and usage. • Cisco Talos and Cognitive Intelligence global threat intelligence research[1]
Firewall Event Data[3]	• Username and/or User ID • Accessed URLs • IP addresses • Event Type • File names[4]	• Enable customer to visualize device events and perform threat detection and analytics on such events. • Cisco Talos and Cognitive Intelligence global threat intelligence research[1]
Endpoint Data[5]	• IP address • MAC address • Operating system • Organizationally Unique Identifier • Fully qualified Domain Name • Host Name • Username	• The customer has the option to elect to send this additional endpoint data to Secure Cloud Analytics for visualization within Secure Cloud Analytics and retention for compliance purposes. • May also be used for security analytics, forensics, efficacy research, general product functionality and usage. logs containing user data for threat detection. • Cisco Talos and Cognitive Intelligence global threat intelligence research[1]

[1] A customer that does not want to share metadata with Cisco Talos or Cognitive Intelligence can request that the transfer of metadata be disabled by submitting a request by email to swatchc-support@cisco.com. See the Cognitive Intelligence Privacy Data Sheet available here for information regarding the processing of personal data by Cognitive Intelligence.

[2] ETA metadata is collected only if generated by the underlying enterprise network equipment.

[3] Firewall Event Data collected only if customer has purchased the Logging Analytics and Detection ("LA") and/or Total Network Analytics and Monitoring ("TA") package(s) of the Security Analytics and Logging suite.

[4] File names collected only if Customer licenses AMP for Networks.

[5] Endpoint data collected from Cisco ISE only if Customer configures the ISE integration within Secure Cloud Analytics configuration settings.

	• DHCP information (such as class identifier) • Browser user agent information (i.e., operating system run by the browser)	

If a customer contacts the Cisco Technical Assistance Center (TAC) for problem diagnosis and resolution, Cisco TAC may receive and process personal data from Secure Cloud Analytics that is provided by customer. The Cisco TAC Service Delivery Privacy Data Sheet describes Cisco's processing of such data. Cisco does not process this data for any other purpose than to assist the customer to resolve issues. For more information, please refer to the Cisco Technical Assistance (TAC) Service Delivery Privacy Data Sheet.

Product usage metrics containing no personal data are collected by Google Analytics on behalf the Secure Cloud Analytics team and are utilized for product analytics and improvement purposes.

3. Data Center Locations

Secure Cloud Analytics leverages third party cloud hosting providers to provide services globally.

Secure Cloud Analytics uses Amazon Web Services (AWS) data centers in the United States, in the European Union and in APJC. A customer may select which region to use for the delivery of the cloud service. Except as provided below, the customer data processed by the cloud service is retained in the selected region. If the APJC data center is selected, then email notifications are sent from the AWS data center in the United States and email addresses and email message contents for portal users are transferred to the AWS data center in the United States to enable such email notifications. If a managed services provider elects to use the Secure Cloud Analytics Partner Portal on behalf of an end customer, Account Information related to Portal Users is transferred to the United States even if the European Union or APJC region is selected because the Secure Cloud Analytics Partner Portal is hosted on AWS in the United States.

As of the publication date of this data sheet, Cognitive Intelligence data centers are located in Europe and Talos data centers are located in the United States. For more information on Cognitive Intelligence, please see the Cognitive Intelligence Privacy Data Sheet.

AWS offers robust controls to maintain security and data protection. Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. The AWS SOC reports provide additional details on the specific control activities executed by AWS. More details can be found at: https://aws.amazon.com/compliance/ and https://aws.amazon.com/security/.

Secure Cloud Analytics Data Centers

Infrastructure Provider	**Infrastructure Provider Locations**
Amazon Web Services (AWS)	• United States - East • United States – AWS GovCloud • APJC - AU • European Union - central (primary) and west (for certain analytics processing)

Talos Data Centers

Infrastructure Provider	**Infrastructure Provider Locations**

Equinix	• United States
Vazata	• United States

4. Cross-Border Data Transfer Mechanisms

Cisco has invested in transfer mechanisms to enable the lawful use of data across jurisdictions:

- Binding Corporate Rules (Controller)
- APEC Cross-Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

5. Access Control

The table below lists the personal data used by Secure Cloud Analytics to carry out the service, who can access that data, and why.

Personal Data Category	Who has access	Purpose of the access
Account Information related to Portal Users	• Customer's Secure Cloud Analytics Portal Users	• Modify and control certain admin data.
	• Cisco	• See "Purpose of Processing" in Section 2 above
Network Flow Metadata	• Customer's Secure Cloud Analytics Portal Users	• Investigating security threats, troubleshooting
	• Cisco	• Deliver, support, upgrade and improve the service. Also see Purpose of Processing in Section 2 above.
Other Metadata	• Customer's Secure Cloud Analytics Portal Users	• Investigating security threats; troubleshooting
	• Cisco	• Deliver, support, upgrade and improve the service. Also see "Purpose of Processing" in Section 2 above.
Enhanced Network Flow Metadata for ETA	• Customer's Secure Cloud Analytics Portal Users	• Investigating security threats; troubleshooting
	• Cisco	• Deliver, support, upgrade and improve the service. Also see "Purpose of Processing" in Section 2 above.
Firewall Event Data	• Customer's Secure Cloud Analytics Portal Users	• Visualization of device events, threat detection and analytics
	• Cisco	• Deliver, support, upgrade and improve the service. Also see "Purpose of Processing" in Section 2 above.
Endpoint Data	• Customer's Secure Cloud Analytics Portal Users	• Data visualization and compliance
	• Cisco	• Deliver, support, upgrade and improve the service. Also see "Purpose of Processing" in Section 2 above.

6. Data Portability

N/A

7. Data Deletion and Retention

The table below lists the personal data used by Secure Cloud Analytics, the length of time that data needs to be retained, and why we retain it.

Type of Personal Data	Retention Period	Reason for Retention
Data Associated with Alerts and Observations	Service alerts and observations are retained throughout the customer's subscription.	Service delivery
Portal User Account Information	Portal user account information is retained throughout the customer's subscription.	Service delivery
Network Flow Metadata, Other Metadata, Enhanced Network Flow Metadata for Encrypted Traffic Analytics, Firewall Event Data, and Endpoint Data	Network flow metadata, other metadata, enhanced network flow metadata for encrypted traffic analytics, firewall event data and logs processed by Secure Cloud Analytics that are not retained in connection with alerts and observations as described above are automatically deleted from the service databases within twelve (12) months.	Service delivery
Data Deletion on Contract Termination or Expiration	Upon expiration or termination of a customer's Secure Cloud Analytics subscription, and except as provided in the column to the right for non-personal information, all data is taken out of processing and a customer's portal account data, data associated with alerts and observations, and all other metadata is purged from the service databases within forty-five days of such expiration or termination, or earlier upon a written request. Some data is stored in encrypted and inactive form in back-ups and is securely deleted within fourteen (14) months.	Certain non-personal information as described below may be retained indefinitely for the following purposes: • Business Analytics: Understand the current state of business, analyze and predict trends, and generate business recommendations. • Product improvement: Monitor product features relevance and usage and suggest engineering points for improvement. The data that may be retained includes alerts and observations statistics (to infer the satisfaction level of each customer), network data (to monitor the size of the customer network), and website telemetry (to profile the users and infer their usage of the web portal). All data that can be used to identify a person is removed from the data set, including but not limited to IP addresses, usernames, and email addresses.
Talos Global Threat Intelligence	All metadata not identified as malware or malicious will be deleted from the Talos databases on a rolling 12-month basis	Network flow metadata and other metadata collected by Talos that are determined to be malware or otherwise malicious are retained indefinitely in the Talos cloud. A customer may request deletion of its metadata in the Talos cloud by opening a Cisco TAC request and/or by submitting a Privacy Request.
Cognitive Intelligence	See the Cognitive Intelligence Privacy Data Sheet available here for information regarding the processing and retention of personal data by Cognitive Intelligence.	

8. Personal Data Security

Cisco has implemented appropriate technical and organizational measures designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure.

Personal Data Category	Security controls and measures
Account Information related to Portal Users	Data is encrypted in transit (TLS 1.2 or later) and at rest (AES 128 encryption or stronger).
Network Flow Metadata	Data is encrypted in transit (TLS 1.2 or later) and at rest (AES 128 encryption or stronger). Talos cloud:

	Data is encrypted in transit (TLS 1.2 or later) and at rest per Talos note below Cognitive Intelligence cloud: Data is encrypted in transit (TLS 1.2 or later) and at rest (AES 128 encryption or stronger).
Other Metadata	Data is encrypted in transit (TLS 1.2 or later) and at rest (AES 128 encryption or stronger). Talos cloud: Data is encrypted in transit (TLS 1.2 or later) and at rest per Talos note below Cognitive Intelligence cloud: Data is encrypted in transit (TLS 1.2 or later) and at rest (AES 128 encryption or stronger).
Enhanced Network Flow Metadata for ETA	Data is encrypted in transit (TLS 1.2 or later) and at rest (AES 128 encryption or stronger).
Firewall Event Data	Data is encrypted in transit (TLS 1.2 or later) and at rest (AES 128 encryption or stronger).
Endpoint Data	Data is encrypted in transit (TLS 1.2 or later) and at rest (AES 128 encryption or stronger).

A note on Cisco Talos: Talos is Cisco's trusted global threat intelligence research team. In order to continually secure Cisco's Security portfolio, certain Security products share data with Talos, which Talos then processes for global threat intelligence research purposes. All data transferred to Talos from Cisco Security products is encrypted in transit. Upon arrival in the Talos data center, such data is in a continuous state of processing to determine whether it includes, or is indicative of, a malicious behavior or activity. If Talos determines the data is not malicious, it is deleted. Any data that is determined to be malicious is retained by Talos, remaining in a constant state of processing, unless Talos determines it is no longer malicious, at which point, it will be deleted. Data within Cisco Talos is encrypted at rest.

9. Sub-processors

Cisco partners with service providers that act as sub-processors and contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for the service is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services ("AWS")	• Account Information related to Portal Users • Network Flow Metadata • Other Metadata • Enhanced Network Flow Metadata for ETA Firewall Event Data	Secure Cloud Analytics is hosted in AWS, and makes use of servers and storage in AWS to implement Secure Cloud Analytics	• United States - East • United States – AWS GovCloud • APJC - AU[6] • European Union - central (primary) and west (for certain analytics processing)
Marketo	• Administrator and trial requestor contact information (name, company, address, email, phone number)	Marketing automation platform containing administrator/requestor contact information. Supplements Salesforce to assist with activation, onboarding, authentication, entitlement, service notifications and inquiries, and customer success purposes	United States - West
Auth0	Username and/or user ID (e.g. email address)	Single Sign On	United States - West
Salesforce	• Administrator and trial requestor contact information (name, company, address, email, phone number)	Customer relationship management platform. Salesforce utilized in the activation, authentication and onboarding process.	United States: Washington D.C., Chicago

[6] APJC – Tokyo for storing firewall log data, shared over encrypted channel with Sydney, AU for LA and TA packages of Security Analytics and Logging.

10. Information Security Incident Management

Breach and Incident Notification Processes

The Information Security team within Cisco's Security & Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. The Incident Commander directs and coordinatesCisco's response, leveraging diverse teams including the Cisco Product Security Incident Response Team (PSIRT), the Cisco Security Incident Response Team (CSIRT), and the Advanced Security Initiatives Group (ASIG).

PSIRT manages the receipt, investigation, and public reporting of security vulnerabilities related to Cisco products and networks. The team works with Customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Cisco products and networks. The Cisco Security Center details the process for reporting security incidents.

The Cisco Notification Service allows Customers to subscribe and receive important Cisco product and technology information, including Cisco security advisories for critical and high severity security vulnerabilities. This service allows Customers to choose the timing of notifications, and the notification delivery method (email message or RSS feed). The level of access is determined by the subscriber's relationship with Cisco. If you have questions or concerns about any product or security notifications, contact your Cisco sales representative.

11. Certifications and Compliance with Privacy Requirements

The Security and Trust Organization and Cisco Legal provide risk and compliance management and consultation services to help drive security and regulatory compliance into the design of Cisco products and services. The Service is built with privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements.
In addition to the Cross-Border Data Transfer Mechanisms/Certifications listed in Section 4, Cisco has the following:

- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework

In addition to complying with our stringent internal standards, Cisco also continually maintains third-party validations to demonstrate our commitment to information security. Secure Cloud Analytics has received the following certifications:

- ISO/IEC 27001:2013 - Information Security Management System (ISMS): An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

- ISO/IEC 27017:2015 - Guidelines for information security controls applicable to the provision and use of cloud services by providing additional implementation guidance for relevant controls specified in ISO/IEC 27002 and additional controls with implementation guidance that specifically relate to cloud services.

- ISO/IEC 27018:2014 - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. Establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment. Specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which might be applicable within the context of the information security risk environment(s) of a provider of public cloud services.

12. Exercising Data Subject Rights

Users whose personal data is processed by the Service have the right to request access, rectification, suspension of processing, or deletion of the personal data processed by the Service.

We will confirm identification (typically with the email address associated with a Cisco account) before responding to the request. If we cannot comply with the request, we will provide an explanation. Please note, users whose employer is the Customer/Controller, may be redirect to their employer for a response.

Requests can be made by submitting a request via:

1) the Cisco Privacy Request form
2) by postal mail:

Chief Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES

Americas Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES

APJC Privacy Officer
Cisco Systems, Inc.
Bldg 80, Lvl 25, Mapletree Biz City,
80 Pasir Panjang Road,
Singapore, 117372
SINGAPORE

EMEAR Privacy Officer
Cisco Systems, Inc.
Haarlerbergweg 13-19, 1101 CH
Amsterdam-Zuidoost NETHERLANDS

We will endeavor to timely and satisfactorily respond to inquiries and requests. If a privacy concern related to the personal data processed or transferred by Cisco remains unresolved, contact Cisco's US-based third-party dispute resolution provider. Alternatively, you can contact the data protection supervisory authority in your jurisdiction for assistance. Cisco's main establishment in the EU is in the Netherlands. As such, our EU lead authority is the Dutch Autoritiet Persoonsgegevens.

13. General Information

For more general information and FAQs related to Cisco's Security and Privacy Program please visit The Cisco Trust Center.

Cisco Privacy Data Sheets are reviewed and updated on an annual, or as needed, basis. For the most current version, go to the Personal Data Privacy section of the Cisco Trust Center.